CLAIMS

WHAT IS CLAIMED:

1. A method, comprising:

determining security information associated with at least one object of a transaction;

determining if a remote device is capable of providing a level of security indicated by at least a portion of the security information; and

transmitting the object to the remote device in response to determining that the remote device is capable of providing the level of security.

2. The method of claim 1, wherein the object is a business object, and wherein determining if the remote device is capable of providing the level of security comprises:

transmitting to the remote device information representative of the level of security that is desired; and

receiving a response from the remote device indicating that the remote device is capable of providing the desired level of security.

3. The method of claim 1, wherein determining the security information comprises accessing a header portion of the object.

4. The method of claim 3, wherein determining the security information comprises determining security information relating to at least one of connection information, class information, trusted entities information, and logging capability information.

5. The method of claim 3, wherein accessing the header portion of the object comprises accessing at least one header of a Simple Object Access Protocol message.

6. The method of claim 1, further comprising determining an alternative remote device that is capable of providing the level of security represented in response to determining that the remote device is not capable of providing the level of security.

7. The method of claim 1, further comprising causing the remote device to execute at least one module that allows the remote device to provide the level of security.

8. The method of claim 1, wherein determining the security information comprises determining the security information in response to receiving the object from a remote device.

9. An article comprising one or more machine-readable storage media containing instructions that when executed enable a processor to:

determine security information associated with at least one object of a given transaction;

receive a response from a remote device indicating that remote device is capable of providing a level of security that is represented by at least a portion of the security information; and

transmit the object to the remote device in response to receiving the response from the remote device.

10. The article of claim 9, wherein the object is a business object, and wherein the instructions when executed enable the processor to transmit to the remote device information representative of the level of security that is desired.

11. The article of claim 10, wherein the instructions when executed enable the processor to access a header portion of the object.

12. The article of claim 11, wherein the instructions when executed enable the processor to determine security information relating to at least one of connection information, class information, trusted entities information, and logging capability information.

13. The article of claim 11, wherein the instructions when executed enable the processor to access at least one header of a Simple Object Access Protocol message.

14. The article of claim 9, wherein the instructions when executed enable the processor to determine an alternative remote device that is capable of providing the level of

security represented in response to determining that the remote device is not capable of providing the level of security.

15. The article of claim 9, wherein the instructions when executed enable the processor to cause the remote device to execute at least one security module to provide the level of security.

16. The article of claim 9, wherein the instructions when executed enable the processor to determine the security information in response to receiving the object from a remote device

17. An apparatus, comprising:

a storage unit having stored therein an object associated with a given transaction; and

a control unit communicatively coupled to the storage unit, the control unit adapted to:

determine security information associated with the at least one object;

determine if a remote device is capable of providing a level of security represented by at least a portion of the security information; and

transmit the object to the remote device in response to determining that the remote device is capable of providing the level of security.

18. The apparatus of claim 17, wherein the control unit is adapted to:

transmit to the remote device information representative of the level of security that is desired; and

receive a response from the remote device indicating that the remote device is capable of providing the desired level of security.

19. The apparatus of claim 17, wherein the control unit is adapted to access a header portion of the object.

20. The apparatus of claim 19, wherein the control unit is adapted to determine security information relating to at least one of connection information, class information, trusted entities information, and logging capability information.

21. The apparatus of claim 20, wherein the control unit is further adapted to determine an alternative remote device that is capable of providing the level of security represented in response to determining that the remote device is not capable of providing the level of security.

22. The apparatus of claim 17, wherein the control unit is further adapted to cause the remote device to execute at least one security module to provide the level of security.

23. The apparatus of claim 17, wherein the control unit is adapted to determine the security information in response to receiving the object from a remote device.

24. A system, comprising:

a first processor-based device adapted to:

determine security information associated with at least one object of a given transaction;

determine if a second processor-based device is capable of providing a level of security represented by at least a portion of the security information; and

transmit the object to the second processor-based device in response to determining that the second processor-based device is capable of providing the level of security; and

a second processor-based device communicatively coupled to the first processor-based device, the second processor-based device adapted to receive the object.

25. The system of claim 24, wherein the second processor-based device is adapted to indicate to the first processor-based device that the second processor-based device is capable of providing a level of security represented by at least a portion of the security information.

26. The system of claim 24, wherein the first processor-based device is adapted to indicate to the second processor-based device the level of security that is desired, and wherein the second processor-based device is adapted to configure itself with at least one module to

provide the desired level of security based on receiving the indication from the first processor-based device.

27. The system of claim 24, wherein the second processor-based device is adapted to:

determine if a third processor-based device is capable of providing a second level of security represented by at least a portion of the security information; and

transmit the object to the third processor-based device in response to determining that the third processor-based device is capable of providing the second level of security.

28. A method, comprising:

receiving, at a first device, a request from a second device desiring to transmit at least one object, wherein the request includes at least a portion of security information associated with the object;

determining if the first device is capable of providing a level of security represented by the security parameter; and

transmitting an indication to the second device based on determining if the first device is capable of providing the level of security.

29. The method of claim 28, further comprising configuring the first device with at least one module that allows the first device the capability of providing the level of security.

30. The method of claim 29, further comprising receiving the data object from the second device.